Exhibit D

Whistleblower: Ubiquiti Breach "Catastrophic"

March 30, 2021 149 Comments

On Jan. 11, **Ubiquiti Inc.** [NYSE:UI] — a major vendor of cloud-enabled Internet of Things (IoT) devices such as routers, network video recorders and security cameras — disclosed that a breach involving a third-party cloud provider had exposed customer account credentials. Now a source who participated in the response to that breach alleges Ubiquiti massively downplayed a "catastrophic" incident to minimize the hit to its stock price, and that the third-party cloud provider claim was a fabrication.

Update, Dec. 5, 2021: The Justice Department has indicted a former Ubiquiti developer for allegedly causing the 2020 "breach" and trying to extort the company.

Original story:

A security professional at Ubiquiti who helped the company respond to the two-month breach beginning in December 2020 contacted KrebsOnSecurity after raising his concerns with both Ubiquiti's whistleblower hotline and with European data protection authorities. The source — we'll call him **Adam** — spoke on condition of anonymity for fear of retribution by Ubiquiti.

“It was catastrophically worse than reported, and legal silenced and overruled efforts to decisively protect customers,” Adam wrote in a letter to the European Data Protection Supervisor. “The breach was massive, customer data was at risk, access to customers’ devices deployed in corporations and homes around the world was at risk.”

Ubiquiti has not responded to repeated requests for comment.

Update, Mar. 31, 6:58 p.m. ET: In a post to its user forum, Ubiquiti said its security experts identified “no evidence that customer information was accessed, or even targeted.” Ubiquiti can say this, says Adam, because it failed to keep records of which accounts were accessing that data. We’ll hear more about this from Adam in a bit.

Original story:

According to Adam, the hackers obtained full read/write access to Ubiquiti databases at **Amazon Web Services** (AWS), which was the alleged “third party” involved in the breach. Ubiquiti’s breach disclosure, he wrote, was “downplayed and purposefully written to imply that a 3rd party cloud vendor was at risk and that Ubiquiti was merely a casualty of that, instead of the target of the attack.”

In its Jan. 11 public notice, Ubiquiti said it became aware of “unauthorized access to certain of our information technology systems hosted by a third party cloud provider,” although it declined to name the third party.

Dear Customer,

We recently became aware of unauthorized access to certain of our information technology systems hosted by a third party cloud provider. We have no indication that there has been unauthorized activity with respect to any user's account.

We are not currently aware of evidence of access to any databases that host user data, but we cannot be certain that user data has not been exposed. This data may include your name, email address, and the one-way encrypted password to your account (in technical terms, the passwords are hashed and salted). The data may also include your address and phone number if you have provided that to us.

As a precaution, we encourage you to change your password. We recommend that you also change your password on any website where you use the same user ID or password. Finally, we recommend that you enable two-factor authentication on your Ubiquiti accounts if you have not already done so.

Change Password Enable Two-Factor Authentication

We apologize for, and deeply regret, any inconvenience this may cause you. We take the security of your information very seriously and appreciate your continued trust.

Thank you,
Ubiquiti Team

In reality, Adam said, the attackers had gained administrative access to Ubiquiti's servers at Amazon's cloud service, which secures the underlying server hardware and software but requires the cloud tenant (client) to secure access to any data stored there.

"They were able to get cryptographic secrets for single sign-on cookies and remote access, full source code control contents, and signing keys exfiltration," Adam said.

Adam says the attacker(s) had access to privileged credentials that were previously stored in the LastPass account of a Ubiquiti IT employee, and gained root administrator access to all Ubiquiti AWS accounts, including all S3 data buckets, all application logs, all databases, all user database credentials, and secrets required to forge single sign-on (SSO) cookies.

Such access could have allowed the intruders to remotely authenticate to countless Ubiquiti cloud-based devices around the world. According to its website, Ubiquiti has shipped more than

85 million devices that play a key role in networking infrastructure in over 200 countries and territories worldwide.

Adam says Ubiquiti's security team picked up signals in late December 2020 that someone with administrative access had set up several Linux virtual machines that weren't accounted for.

Then they found a backdoor that an intruder had left behind in the system.

When security engineers removed the backdoor account in the first week of January, the intruders responded by sending a message saying they wanted 50 bitcoin (~$2.8 million USD) in exchange for a promise to remain quiet about the breach. The attackers also provided proof they'd stolen Ubiquiti's source code, and pledged to disclose the location of another backdoor if their ransom demand was met.

The intruders responded by sending a message saying they wanted 50 bitcoin (~$2.8 million USD) in exchange for a promise to remain quiet about the breach.

Ubiquiti did not engage with the hackers, Adam said, and ultimately the incident response team found the second backdoor the extortionists had left in the system. The company would spend the next few days furiously rotating credentials for all employees, before Ubiquiti started alerting customers about the need to reset their passwords.

But he maintains that instead of asking customers to change their passwords when they next log on — as the company did on Jan. 11 — Ubiquiti should have immediately invalidated all of its customer's credentials and forced a reset on all accounts, mainly because the intruders already had credentials needed to remotely access customer IoT systems.

"Ubiquiti had negligent logging (no access logging on databases) so it was unable to prove or disprove what they accessed, but the attacker targeted the credentials to the databases, and created Linux instances with networking connectivity to said databases," Adam wrote in his letter. "Legal overrode the repeated requests to force rotation of all customer credentials, and to revert any device access permission changes within the relevant period."

If you have Ubiquiti devices installed and haven't yet changed the passwords on the devices since Jan. 11 this year, now would be a good time to take care of that.

It might also be a good idea to just delete any profiles you had on these devices, make sure they're up to date on the latest firmware, and then re-create those profiles with new [and preferably unique] credentials. And seriously consider disabling any remote access on the devices.

Ubiquiti's stock price has grown remarkably since the company's breach disclosure Jan. 16. After a brief dip following the news, Ubiquiti's shares have surged from $243 on Jan. 13 to $370 as of today. By market close Tuesday, UI had slipped to $349. Update, Apr. 1: Ubiquiti's stock opened down almost 15 percent Wednesday; as of Thursday morning it was trading at $298.

This entry was posted on Tuesday 30th of March 2021 02:00 PM

A LITTLE SUNSHINE | DATA BREACHES | UBIQUITI BREACH | UBIQUITI INC. | UBIQUITI NETWORKS

149 thoughts on “Whistleblower: Ubiquiti Breach “Catastrophic””

Joe S.
March 31, 2021
I wonder how their Amplifi product line is affected by this. You can use different methods including your Facebook login to manage your AP remotely. I ended up removing this ability and resetting my Facebook password just in case. I also disabled the remote VPN (Teleport) as well.

Darwin
-
April 6, 2021
You would use Facebook to log into a router??

tmcg
March 31, 2021
I wonder how much this “informant” shorted the companies stock?

Anon
-
March 31, 2021
You’re kidding right? Krebsonsecurity is better than that.

tmcg
-
March 31, 2021
Not kidding at all and this is not a knock on Krebsonsecurity in any way but look at the stock price. It hits an all time high (with plenty of room to drop) and then the informant drops this news. Again not saying UI didn’t do something wrong… but with this knowledge and good timing Im sure Mr. Anonymous is sitting pretty well.

Chaos215bar2
-
March 31, 2021
I see. And obviously you must work for Ubiquity’s PR team, or otherwise have a vested interest in the company. Because, what other possible motivation could you have for casting doubt on the whistleblower’s motivations like that? (See how this works?)

Bryn
-
March 31, 2021

Because burden on proof is on the person that is making the claim? Literally Debating 101

Baer

-

April 1, 2021

All these devout krebbsies… Just because Krebs would post the story doesn't validate or invalidate Krebs and it shouldn't cause you to validate or invalidate the whistleblower. Simply start with the data, just because your favorite blogger would post something doesn't now mean that a human wouldn't take advantage for selfish gain and end up fluffing the story more than necessary.

Kenny

-

April 8, 2021

UBNT validated Krebs when they acknowledged the article

Wu-Tang Fo-Eva!

-

April 1, 2021

Come on. Yall acting like the WB had any other motivation that profit. gtfoh..C.R.E.A.M!!

JamminJ

-

April 1, 2021

People who accuse whistleblowers are often projecting their own lack of morals.

Many security professionals here are very passionate about their work and get significantly upset when their management rejects sound guidance.
It's even more upsetting when they flat out lie.

So if you were a professional, an expert in your field, and some lawyer or executive contradicts your expertise… Lying about the facts.
You would probably also have plenty of motivation to blow the whistle too.

Bubba

-

April 4, 2021

Truer words…

PandaBear

-

April 5, 2021

I work at Ubiquiti currently and am about 99% certain who the whistleblower was. He owned no stock – he was passionate about security, ignored and scrutinized by CEO and his peers at the company. There is no "management" at Ubiquiti, everyone just gets micromanaged by the CEO essentially.

JamminJ

-

March 31, 2021

That would be criminal, stupid, and criminally stupid.

Since he was involved with response to this breach, that association with the company, whether as an employee, contractor, or temp… legally that's an "insider".

So although he could hold a position in the stock… anything like buying or short selling stock during the last few months… would immediately put him under severe liability for insider trading.

This isn't the case of some outsider, blogger, or pundit making wild claims anonymously or under a pseudonym in order to move a stock. This is someone with inside knowledge, and thus subject to strict regulations.

Matt

-

March 31, 2021

Sure, and maybe while we're wildly speculating, the whistleblower was involved in the attack too? I mean, its possible right?

The lawyers and execs always try to do damage control. ALWAYS. Sometimes they do the the right thing (or at least contain their spin) because they have some ethics, sometimes it's more about the fear of getting caught. The SEC should investigate and if this crap is true, rip Ubiquiti a new one so the rest of the lawyers and execs without ethics at least have something to fear.

d

-

April 2, 2021

Slow down there, guy. That's too much critical thinking. In America, we just need to stay in line and keep going to work.

Nicole Price

-

March 31, 2021

Pretty sure he means "Adam"

Simon

-

April 1, 2021

He meant the whistle blower shorted the company, not Brian.

AnonBox

-

April 1, 2021

That would be really dumb. Given his position he would be marked as an insider for a publicly traded company. I'm marked as one for a company (just a normal worker) and you can only trade during a set window, which is clearly stated. Also derivatives and shorting are a no no. He would be easily caught.

I really doubt anyone would go, "Gee, this company I work for, let me know short it and release damaging information". Not only that he probably has RSUs like most tech employees. So he would have to short more than the loss he takes on RSUs, which would be substantial enough to

draw red flags. He obviously wasn't thinking about share price and actually concerned about the response.

AnonBox

-

April 1, 2021

Sorry, posted twice. Thought it didn't go through the first time

dealer

-

April 1, 2021

100% agree, CS has hold shome short p. for one of their shady customer

dealer

-

April 1, 2021

relax everything fine. CS has holds some short p. for their shady customer

Custon keto diet

March 31, 2021

It's no big surprise that individuals would go to this arrangement rather than items that have hazardous energizers.

Joe

March 31, 2021

Since the source code was part of the dump, and signing keys exfiltrated, were their repositories scanned for unauthorised changes? Were malicious firmware updates published in the official feed?

stu

March 31, 2021

ubiqiti two factor auth is crap. it doesn't allow you to change your phone. it should be assigned to a phone number, not a phone. after i changed my phone, i couldn't access my account. change it please.

laplaces_futon

-

March 31, 2021

@stu, the 2 factor auth method ubiquiti uses is the open "Time-Based One-Time Password Algorithm" described in RFC 6238, which is implemented in the most common 2FA apps (Google Authenticator, Microsoft Authenticator), and used widely by service providers, including facebook, amazon, the google, paypal, and microsoft, to name only a few big'uns.

The central idea here is that it *must* be impossible to perform 2FA without the one phone that contains the secret key shared by you and the provider.

When a user registers 2FA at ubiquiti, they are given the opportunity to save 10 one-use passcodes that can be used to authenticate if the "one phone" is lost or unavailable, allowing 2FA to be moved to a new device if desired.

It's a good idea to get those passcodes and save them somewhere safe–electronically in a secure password manager, or on paper in a secure location–so that a damaged or missing phone is not a denial of service attack.

Yyz

-

April 1, 2021

Or use Authy instead of Google or Microsoft Authenticator apps. Authy let you sync your TOTP codes across multiple devices.

Jhon

-

April 2, 2021

MS Authenticator also lets you sync across multiple devices.

Jhon

-

April 2, 2021

Clarification – MS Authenticator lets you back up all of your TOTP codes to your Microsoft account, so that you can restore them to other devices. MS is storing your TOTP configuration so that you're not required to rely on any other devices.

JamminJ

-

April 2, 2021

So when Microsoft is breached again…

TheWired

-

April 7, 2021

Realistically, MS storing your TOTP configurations is better then most people's cell phones. so… It's a more of a question of which is the easier target, with the more lucrative prize? unless I have a massive team behind me or state funding, I'm probably not going to try to attack MS's servers for those TOTP configurations, I rather try to lift someone's phone and work on that to gain access to their data that way.

JamminJ

-

March 31, 2021

What you're suggesting is the opposite of secure 2FA.

Binding to a phone number instead of the phone device itself… is exactly why SMS as 2FA is so insecure.

I'm glad you lost access to your account after you changed your phone. Because that's precisely what a malicious attacker would do to steal your account. Social Engineering, just say the phone has changed.

Good 2FA should have the 2nd factor be an actual physical device in your possession, not an abstract identity that can be transferred on the whims of minimum wage employees sitting at the

helpdesk, like at the cellular carrier.

Hampton DeJarnette

March 31, 2021

For Daniel Geer readers:
Geer's column in the March/April issue of "IEEE Security & Privacy" references this Brian Kreb's article": "https://krebsonsecurity.com/2019/10/avast-nordvpn-breaches-tied-to-phantom-user-accounts".

Hennie

March 31, 2021

I am simply awe-struck and speechless…
I spent literally months trying to figure out why our newly formed domain and everything that was dependent on the previous domain – (which was hacked by our chief financial officer's cyber criminal friends and gained access to passwords and credentials and spoofing my email correspondence causing defamation cases and theft of company funds worth millions) didn't work as expected after upgrading all our infrastructure to the latest UniFi products …
And to rely on lawyers and corrupt police officials to bring the perpetrators to book simply drained millions more…
But thank goodness that the truth will always prevail…
Let's put these criminals behind bars in jail cells infested with a colony of bats from the chemical warfare labs in China.

Wow

-

April 1, 2021

You're justifying torture, implying an act of war committed on the world by China, and all because you had a couple of technical issues? I'm simply awe-struck and speechless.

Hoe

-

April 1, 2021

Are you totally trembling and completely triggered? Somebody said something on the internet? You poor person.

Darwin

-

April 6, 2021

You're an idiot.

HM Visser

-

April 12, 2021

It was my personal experience and I am sure – had you been in my shoes and lost millions of your own money pumped into a business for 35 years – you would feel the same. I treated the culprits with the utmost respect and they earned above average salaries with benefits like company cars and fuel..yet they decided to rather steal and commit fraud. Subsequently I found

out they did it before at various other companies, and always managed to get off the hook by serving very light jail sentences or bribing officials and extorting lawyers by digging up dirt on them.

So please, if you feel these are merely “technical issues” and that I am a “war monger” against a country – who also has absolutely no regard for cybersecurity or IP rights – you are indeed an idiot….

SgtChains

April 1, 2021

Given that in 2019 Ubiquiti was seen slurping up data from deployed devices without informing those that had purchased their equipment, it kind of puts this into a different light.

https://www.theregister.com/2019/11/07/ubiquiti_networks_phone_home/

Mochas

April 1, 2021

I am just here for the comments.

Ccinos

-

April 1, 2021

Is that how this works? Sign me up, too.

Taylor

April 1, 2021

I’m curious if in other organizations legal has this kind of power over things like forcing password resets. That has nothing to do with legal in any way shape or form. Once again, attorney’s are the problem. Also, as in many organizations, they wait for something terrible to happen before they finally secure their systems correctly.

Quid

-

April 1, 2021

Don’t forget the bean-couting accountants too and ultimately the
C-level management that apparently has no clue about doing the “right thing” other than what the lawyers and accountants tell them.

Jhon

-

April 2, 2021

Legal and business people obviously have an obligation to customers that entrust them with their security – but they also need to ensure the survivability of the company and ultimately they are responsible if a company fails. When there are downturns in business, they are the ones that have to make the decisions to lay people off. For the vast majority of attorneys and business leaders, these are actually terrible decisions to make. Nobody wants to be in that position.

Something you need to understand about situations like this is that doing the right thing is not as easy as complying with the law 100% or protecting customers at all costs. I’m sure this will be

really controversial, but please, read my basic explanation and seek to understand. It's a situation of the lesser of multiple evils. Sometimes, business leaders/lawyers are faced with a situation were there is no good decision to make – all paths will have negative consequences, and you need to choose the path (based on risk, impact, etc.) that will probably have the least negative consequences. These decisions are a very complex combination of risks.

Part of the decision as it relates to compliance is to factor in the probability and impact of any noncompliance. That doesn't sound right, but it's a product of being a business, not a product of bad humanity. That's why compliance requirements have specific consequences for noncompliance. It's why GDPR has set such outrageous fines for noncompliance – because they know (yes, even in the EU) that businesses have to factor in the consequences of noncompliance in their decisions.

Since Adam has apparently contacted the EU DPB about this, let's go into more detail on the risk to the privacy of Ubiquiti's customers. Under GDPR, not all breaches have to be reported (really). A breach only needs to be reported if there is a high likelihood of a serious risk to the privacy/rights/security of an individual. In this specific case, what information did Ubiquiti's lawyers and business leaders have to support the probability of serious risk to its customers? And whose responsibility was it to collect that information? Most likely, it was IT that should have set up and enabled logging on the data that was accessed (seriously, this is not a C-Suite decision, this is a much lower-level decision). But because IT did NOT configure their systems to create these types of logs, the business leaders didn't have crap to go on. They literally had no credible information to support a position that any specific customers' data was actually accessed. It could have been, and we can speculate about this all day, but unless we see hard data appear on the dark web, nobody will have any information to support their position. In the absence of this info, the only thing we can conclude is that IT was not able to provide the business leaders with any information to support a claim that individuals' information was actually compromised. And that's part of what makes this a very terrible decision for the business leaders to have to make. They have to weigh the impact of very severe consequences to their company (and their employees) against the *potential* impact to their customers. So do you see how this ended up playing out the way it did at Ubiquiti?

Take this another step further. We know there was an extortion attempt after the hacker realized they had been discovered, right? If the attacker really had the keys to the kingdom and had exfiltrated all of their customers' information and could take down all of their customers networks, they wouldn't have stopped with a single ransom demand, would they? No. No way. At the very least, the attacker would start posting bits of information on the dark web to support their claim and pursue the ransom demand, or else sell that information on the dark web to get some value from it. I haven't heard any indications of that, and it's been almost three months since that initial extortion attempt. What does that tell you?

My bet is that this breach is probably going to play out to be a big nothingburger. Otherwise, something else would have already happened by now.

JamminJ

-

April 2, 2021

That right there is a great nuanced analysis, and I can attest is VERY accurate in medium/large corporate environments.

People are quick to play Monday Morning Quarterback, and pretend like they could do better if they were in charge. Reality is so nuanced and complicated. Without shifting blame or excusing failings, it is possible to understand how things like this keep happening.

BTW, the very next sentence in this article after the mention of ransom…
"The attackers also provided proof they'd stolen Ubiquiti's source code"
Now, source code doesn't fall under the protections of data privacy, so your point is still correct about the likely conflict between legal and IT.

Gabe

-

April 2, 2021

I agree with most of what you say, including that it seems unlikely that they exfiltrated customer credentials if we haven't seen evidence of it by now. However, if what the WB says is true—AWS root credentials and no internal logging—then Legal took a huge bet and dodged a bullet, and I would consider them grossly negligent. As a networking company, there needs to be a high bar for security, and the CTO or CISO needs to push back on Legal (who don't understand what AWS root actually means) and tell them that this is a reputation destroying event for a company that made their bones on making high quality prosumer gear whose rise to prominence was driven by alpha geeks.

TenYearTexan

-

April 5, 2021

I see some nuance in Jhon's response (the main benefit being to point out that not every intrusion is successful and it doesn't serve anyone to take drastic actions until there is reason to believe major damage was done. cry wolf etc).

I still view the actions of Ubiquiti with some anger. Laws are in place to force people to take actions that go against the innate motivations of self-preservation and profit. The fact that there was other operational mistakes (no logging, no IDM, no stored data encryption, inadequate segmentation of information etc) which prevents the company from properly evaluating the risk should mean that they default to assuming a larger risk for their customers, not hoping it's a small risk and waiting to see severe damage before warning other customers of such damage. (hurricane warnings, hit-n-run laws are the examples I'd reach for).

I don't know the details of the GPDR law. If it was well-written, it will include allow flexibility to cover companies large and small for intrusions large and small, but the point of the legislation is to force companies to promptly and clearly inform the public if there is any risk of major loss. From the details shared, there IS such a risk. The coy press release in my view was an attempt to shift blame to a third party for multiple Ubiquiti operational failures and an obfuscation of the true potential threat. Secondly, the public and the law don't care about who and how departments failed – the company as a whole bears the responsibility. I love Ubiquiti gear – cheaper and more functional than competitors IMHO, but I hope that they are penalized for their inadequate response (poor legal team decisions imho).

(BTW, I appreciate devils-advocate posts like Jhon's to encourage intellectual and not emotional reactions. As background for good internal processes, such info is great, but these points don't change my mind on liability and crisis response in this situation).

Mike

April 1, 2021

Lol, i hope the hackers drop their own firmware updates to everyone's Unms appliances. We'll know its happened when all the edge routers start working reliably, for the first time ever ever.

JT

April 1, 2021

Maybe this is coincidence, but I have a support case open with Ubiquiti now because the last 2 Unifi Controller releases are signed with an expired certificate. It is especially odd because prior releases were signed correctly, sounds like something is broken in the build process. Possibly as a result of this breach?

Tomato

-

April 1, 2021

Rut ro. There's no open firmware for these devices rigth?

Stephen

-

April 1, 2021

That could be dangerous if you imagine an attack similar to the SolarWinds breach

MCB

April 1, 2021

"Such access could have allowed the intruders to remotely authenticate to countless Ubiquiti cloud-based devices around the world."

Please elaborate. Are you saying that Ubiquiti can initiate logins to customer controllers? I thought the controllers were initiating the communication to the UniFi cloud, allowing a reverse proxy, but not storing controllers' credentials in the UniFi cloud.

PG

-

April 1, 2021

With access to the source code and all the cryptographic keys pretty anything is possible.

Facticious

-

April 2, 2021

Again, please elaborate?
In a salty one-way encryption situation, how exactly would they log in to my gear?

- UNIVERSITY_SOC

-

April 2, 2021

Its what's known as a "Back door". I don't know if anyone here has ever heard of em.

d

-

April 2, 2021

tickets.cgi on any airos device.
I won't say more; but dig deep and the truth will surprise you 🙂

Nick

-

April 3, 2021

Well, they had the signing keys for the firmware and access to the backend so if devices auto update they could have just pushed modified firmware that did anything

I'm not super familiar with how Ubiquiti's cloud products work but presumably they have a button somewhere to apply firmware updates so devices would happily go along and update to whatever signed blob is available

joshua stein

April 2, 2021

Did the company have a CISO prior to the breach? I am curious what their security program was like… I do see they posted a CISO position on their careers page post-breach. That now appears to have been filled (assumption, given the job post has been removed from the careers page). Ubiquiti is a billion dollar company. To not have a solid security program is one thing (very bad). To be selling networking and "security" products and not have a solid security program is IMO negligent.

There are still multi-billion dollar companies that have little-to-no security program, no one leading security, etc. Publicly traded too. Icing on the cake is some sell sell products that could impact health & safety, property, life, and classified information. Absolutely crazy that there is no accountability.

JamminJ

-

April 2, 2021

They probably had a security program and a chief security officer. It's not uncommon to have the CISO fired or quit after a major breach like this.

Marcu

April 2, 2021

Does this mean that all Ubiquiti devices need to be viewed as compromised? I have a Unifi cloud controller that is running in a VM and I naively connected it to the Ubiquity cloud login to use the app on my phone.
Reading about the scale of this breach has me seriously concerned that anything connected to the controller is possibly compromised. I have updated the controller and device firmware since the breach was announced initially and the fact that the signing keys were compromised has me really worried.

Do I have any choice other than throwing out all Ubiquity gear and starting over with a different brand?

Hiland

April 3, 2021

In early March I installed an AMPLIFI system. I signed up for a Ubiquity account using my Apple account.

Within minutes, I was getting multiple requests for my 2FA token for my Apple account. It kept happening until I changed my Apple password.

At the moment I thought it was a coincidence, but now I wonder how compromised my network is.

Igor Levicki

April 4, 2021

I only need to know one thing — were the update servers compromised?

Between the date the breach happened and now, people could be running backdoored firmwares and UniFi Controllers without knowing it and if so, changing a few passwords won't help them at all.

At the very minimum, Ubiquiti needs to publish verifiably secure firmware and software updates signed with a new set of signing keys.

suneg

-

April 11, 2021

Spot on Igor. Should a malicious firmware have been pushed, you might as well throw out your gear. I mean .. compromised firmware is about as bad as it gets. You can hit "Upgrade firmware" for your controllers/APs/etc. to get new firmware and freshly generated signing keys, but if your device was already compromised, a clever adversary could simply make sure the device appeared as being updated, and never really install the new firmware. Alternatively; modify the new firmware to inject a backdoor, and skip the signature verification process. Just about anything is possible once they're in your firmware.

Perhaps such an approach could be done even without compromising the update servers. If your controller has remote mgmt enabled, I wonder if an adversary would be possible to connect to it, and have it download updated firmware from a non-official feed, but signed with the official keys.

Adrian

April 5, 2021

Here is another Data breach that is Facebook data leak of 533 millions of users, you can read this article to get more insight about this breach
https://wholovehacking.blogspot.com/2021/04/hackers-released-facebook-users-leaked.html

Lisa

April 5, 2021

This is not their first rodeo. Ubiquiti has quite the track record of security incidents: https://en.m.wikipedia.org/wiki/Ubiquiti

giz
April 6, 2021

it seems the sharpest criticism comes from this
“Ubiquiti had negligent logging (no access logging on databases) so it was unable to prove or disprove what they accessed, but the attacker targeted the credentials to the databases, and created Linux instances with networking connectivity to said databases,” Adam wrote in his letter. “Legal overrode the repeated requests to force rotation of all customer credentials, and to revert any device access permission changes within the relevant period.”

negligent logging on databases -> unable to prove or disprove what they accessed with the implication that Ubiquiti leveraged this fact to indicate they had no proof of access, but access could be reasonably assumed SO Adam thinks at this point customers should be instructed to change passwords, HOWEVER, Ubiquiti was ALSO aware of a second, but not yet discovered, back door

Does it really make sense then to change passwords WHILE the probability of a second, unclosed backdoor exists?
I feel it makes more sense to send the password change notification after the door was closed AND/OR after internal employees reset their passwords

Otherwise the newly changed customer passwords would ALSO be compromised.

What is the timing of the second back door being closed/internal passwords changed as related to the customer bulletin?

me
April 7, 2021

use Ligowave

Ron
April 8, 2021

Is there a definitive answer to there has been no UBNT supply chain problems because they have no clue how long the guys were lurking on their systems?

Michael
April 9, 2021

From https://community.ui.com/questions/Update-to-January-2021-Account-Notification/3813e6f4-b023-4d62-9e10-1035dc51ad2e

“Update to January 2021 Account Notification

As we informed you on January 11, we were the victim of a cybersecurity incident that involved unauthorized access to our IT systems. Given the reporting by Brian Krebs, there is newfound interest and attention in this matter, and we would like to provide our community with more information.

At the outset, please note that nothing has changed with respect to our analysis of customer data and the security of our products since our notification on January 11. In response to this incident, we leveraged external incident response experts to conduct a thorough investigation to ensure the attacker was locked out of our systems.

These experts identified no evidence that customer information was accessed, or even targeted. The attacker, who unsuccessfully attempted to extort the company by threatening to release stolen source code and specific IT credentials, never claimed to have accessed any customer information. This, along with other evidence, is why we believe that customer data was not the target of, or otherwise accessed in connection with, the incident.

At this point, we have well-developed evidence that the perpetrator is an individual with intricate knowledge of our cloud infrastructure. As we are cooperating with law enforcement in an ongoing investigation, we cannot comment further.

All this said, as a precaution, we still encourage you to change your password if you have not already done so, including on any website where you use the same user ID or password. We also encourage you to enable two-factor authentication on your Ubiquiti accounts if you have not already done so.

Thanks,

Team UI”

Comments are closed.